



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/506,765

04/14/2005

Yongmao Li

470061.401USPC

8915

500 7590 05/14/2009

SEED INTELLECTUAL PROPERTY LAW GROUP PLLC  
701 FIFTH AVE  
SUITE 5400  
SEATTLE, WA 98104

EXAMINER

OKEKE, IZUNNA

ART UNIT

PAPER NUMBER

2432

MAIL DATE

DELIVERY MODE

05/14/2009

PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/506,765	LI ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	IZUNNA OKEKE	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

#### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 03 March 2009.
- 2a) ☒ This action is **FINAL**.                      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-26 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-26 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All    b) ☐ Some \*    c) ☐ None of:
1. ☒ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)          | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____  | 6) <input type="checkbox"/> Other: _____                          |

**DETAILED ACTION**

***Response to Arguments***

1. Applicant's arguments filed 03/03/2009 have been fully considered but they are not persuasive.

On Page 1 of applicant's arguments and remarks, applicant argues that Halasz does not disclose an ACCESS\_ACCEPT message sent by the authentication server in response to an authentication request. Although Halasz does not explicitly recite "ACCESS\_ACCEPT", Halasz does disclose a message response to an authentication request (accept/reject, pass/fail) which is known in the art of authentication protocols in response to an authentication access request (See Halasz, Col 6, Line 33-42 and Col 4, Line 58-64 discloses an authentication message (accept/reject, pass/fail) from the authentication server in response to an authentication access request). This authentication response message indicates whether the authentication was successful and hence, accepted, or was not successful and rejected. The examiner interprets this authentication response message as the ACCESS\_ACCEPT message from the authentication server.

Applicant further argues that Halasz is non-analogous art and does not teach the solution of claim 1 which combines the process of distributing encryption key and mobile client authentication. Halasz is analogous art to applicant's claimed invention, it is directed to providing a trust relationship in an 802.1X network between an access point, mobile client and authentication server wherein the mobile client is authenticated by the authentication server and an encryption key (session key is generated for the mobile client and transmitted to the mobile client for encrypting and decrypting communication to and from the access point.

Art Unit: 2432

On Page 2, applicant agrees that an encryption key is obtained for the client but argues that the Authentication Server does not send a message comprising access\_accept information. This has been clarified above; the examiner interprets the authentication response message (pass/fail) as the ACCESS\_ACCEPT message. Halasz further teaches in Col 4, Line 28-31 that the AP derives a session key for the client in the same way the AP obtained the session key in Col 6, Line 35-42 where the Authentication Server derives the key from the client information included in the request message and the mobile client obtains the encryption key if its authentication state or result is successful.

***Claim Rejections - 35 USC § 102***

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-5, 10, 15, 20, 25 and 26 are rejected under 35 U.S.C. 102(b) as being anticipated by Halasz et al. (US-7325246).

a. Referring to claim 1:

Regarding claim 1, Halasz teaches a method for distributing encryption keys in a Wireless Local Area Network (WLAN), comprising: receiving, by an authentication device, an authentication request containing identification information for identity authentication from a mobile host (Col 6, Line 17-33 teaches the wireless client sending an authentication request containing identification information to the AS); authenticating said mobile host according to said identification information; if authentication

Art Unit: 2432

fails, sending a message comprising ACCESS\_REJECT information to said mobile host, and if authentication succeeds, sending a key-related information M1 to an access I point (AP) and a message comprising ACCESS\_ACCEPT information to said mobile host (See the response to argument and Col 6, Line 17-47 teaches the mobile client sending identification information in an authentication request to the AS, the AS authenticating the mobile client and sending an authentication failed notification if the authentication fails and an authentication pass notification if the authentication is successful),

wherein if a key-related information M2 is comprised in said message comprising the ACCESS\_ACCEPT information, said message comprising the ACCESS\_ACCEPT information is encrypted (Col 4, Line 38-64 and Col 6, line 34-58 teaches encryption of the authentication status message and communication between the AS and AP using conventional encryption methods);

said key-related information M1 is used to obtain a key by said AP, said message comprising the ACCESS\_ACCEPT information is used to obtain the key by the mobile host (Col 6, Line 33-43 teaches the AP obtaining a key from the AS based on the client information included in an authentication request and Col 4, Line 25-31 teaches the client obtaining the session key based on the outcome of the authentication request).

a. Referring to claim 2:

Regarding claim 2, Halasz teaches the method for distributing encryption keys in the WLAN of claim 1 wherein said key-related information M1 is the corresponding property information searched by said authentication device according to the identification information (Col 3, Line 36-57 teaches key related information as the identification information searched by

Art Unit: 2432

the AS in the database), the method of said AP obtaining the key comprises:

generating the key according to said property information with a key generation algorithm; and

the method of said mobile host obtaining the key comprises (Col 3, Line 36-57 teaches generating the key according to the identity information with conventional encryption algorithm) :

generating the key according to the property information stored in the mobile host with the same key generation algorithm after said mobile host receives said message comprising the

ACCESS\_ACCEPT information (Col 4, Line 24-37 teaches deriving a key for the wireless client in the same way the AP key was generated after the wireless client goes through successful authentication).

a. Referring to claim 3:

Regarding claim 3, Halasz teaches the method for distributing encryption keys in the WLAN of claim 1 wherein said key-related information M1 is the corresponding property information searched by said authentication device according to the identification information (Col 3, Line 50-57 teaches the key related information as the identity information); the method of said AP obtaining the key comprises:

generating the key with a key generation algorithm; said key-related information M2 is said key generated and encrypted by said AP is sent to said mobile host along with said

ACCESS\_ACCEPT message, said mobile host obtaining the key through decrypting information M2 with said property information (Col 4, Line 24-57 teaches deriving a key by conventional algorithms for the wireless client in the same the AP key was derived).

a. Referring to claim 4:

Art Unit: 2432

Regarding claim 4, Halasz teaches the method for distributing encryption keys in the WLAN of claim 1 wherein said key-related information M1 is the key generated from said property information corresponding to the identification information contained in said authentication request by said authentication device with a key generation algorithm (See the rejection in claim 1), the method of said mobile host obtaining the key comprises: generating the key according to said property information stored in the mobile host with the same key generation algorithm after receiving said ACCESS\_ACCEPT message (See the rejection in claim 1, {deriving the key from the identity information}).

a. Referring to claim 5:

Regarding claim 5, Halasz teaches the method for distributing encryption keys in the WLAN of claim 1 wherein said information M1 and M2 are the key generated from said property information corresponding to the identification information contained in said authentication request by said authentication device with a key generation algorithm, said information M2 is encrypted with said property information and then sent to said mobile host along with said ACCESS\_ACCEPT message, the method of said mobile host obtaining the key comprises:

decrypting said information M2 according to the property information stored in the mobile host after receiving said ACCESS\_ACCEPT message (See the rejection in claim 1. {AP develops relationship and in the process, a key, with the AS after receiving the first identity information. AP develops another trust relationship with the wireless client including a key for the client in like manner with the identity information}).

a. Referring to claim 10:

Art Unit: 2432

Regarding claim 1, Halasz teaches the method for distributing encryption keys in the WLAN of claim 1 wherein said authentication device is an authentication server installed in said external network (See Fig 1a. AS 106).

a. Referring to claim 15:

Regarding claim 15, Halasz teaches the method for distributing encryption keys in the WLAN of claim 1 wherein said authentication device is a wireless gateway that connects said AP with external network (See Fig 1a, Switch and authenticator 100).

a. Referring to claim 20:

Regarding claim 20, Halasz teaches the method for distributing encryption keys in the WLAN of claim 1 wherein said authentication device includes said wireless gateway and said authentication server installed in external network (See Fig 1a, AS 106 and Switch and authenticator 100).

a. Referring to claim 25:

Regarding claim 25, Halasz teaches an authentication device, comprising: a receiving module configured to receive an authentication request from a mobile host, said authentication request comprising identification information for identity authentication (Col 3, Line 6-23 teaches the authenticator of the AS 106 as a receiving module for receiving authentication request comprising identity information);

an authentication module configured to authenticate said mobile host according to said identification information (Col 3, Line 6-23.... Authentication Server 106);

a sending module configured to send a message comprising ACCESS\_REJECT information to said mobile host if authentication fails, and send key-related information M1 to an access point



Art Unit: 2432

(AP) for said AP to obtain a key according to said key-related information M1 and a message comprising ACCESS\_ACCEPT information to said mobile host for said mobile host to obtain the key according to said message comprising the ACCESS ACCEPT information if authentication succeeds (See the rejection in claims 1 and 2).

a. Referring to claim 26:

Regarding claim 26, Halasz teaches a system, comprising: a mobile host, an authentication device, and an access point (AP); said authentication device configured to receive an authentication request from said mobile host, said authentication request comprising identification information for identity authentication, to authenticate said mobile host according to said identification information, to send an ACCEPT\_ACCESS REJECT message to said mobile host if authentication fails, to send a key-related information M1 to an access point (AP), and to send a message comprising ACCESS\_ACCEPT information to said mobile host if authentication succeeds (See the rejection in claim 1 and Figs, 1a and 1b and Col 3-6 teaches a system comprising a wireless client, and AP and AS configured to receive auth request from the client comprising identity information. The AS authenticating the client based on the identity information and sending a reject or accept message with identity information for deriving a key for the wireless client);

said mobile host configured to send an authentication request containing identification information for identity authentication and to obtain a key according to said message comprising the ACCESS\_ACCEPT information; and said AP configured to receive said key-related information M 1 and obtain the key according to said key-related information M1 (See the rejection in claim s 1 and 2).

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 6-9, 11-14, 16-19 and 21-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Halasz et al. (US-7325246), and further in view of Mizikovsky et al.(US-6853729).

a. Referring to amended claim 6:

Regarding claim 1, Halasz teaches the method of distributing encryption keys in the WLAN of claim 1.

Halasz does not explicitly teach the method of distributing keys in a WLAN as outlined in the steps of (a1) to (e1).

However, Mizikovsky teaches the steps of (a1) to (e1).

(a1) said AP generating a random number and generating a new key from said random number with any key generation algorithm (See Mizikovsky, Col 10, Line 33-49 teaches the system generating a random number and generating a key from the random number);

(b1) said AP adding said random number to a key update message and then sending said message to said mobile host (See Mizikovsky, Col 10, Line 33-50 teaches providing a key update message which includes a random number to the mobile unit);

(c1) when receiving said key update message, said mobile host generating a new key from said random number contained in said key update message with the same key generation algorithm as

Art Unit: 2432

that in step (a1) (See Mizikovsky, Col 11, Line 10-14 teaches receiving the update key message and generating the new key in a manner used by the system to generate the key);

(d1) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed (See Mizikovsky, Col 12, Line 17-54 teaches communications between the unit and the system encrypted with the encryption key and the unit. An encryption identifier, the encryption key is included in the message and the encryption key is changed whenever there is a key update); and

(e1) when receiving the data packets from said mobile host, said AP determines whether to change the key value of said encryption identifier (See Mizikovsky, Col 12, Line 39-43 teaches between the mobile node and the system and Line 47-50 further teaches the system determining whether to update the key value based on certain criteria).

Therefore it would have been obvious to one of ordinary skill at the time the invention was made to modify Halasz's system to include the steps of (a1) to (e1) as taught by Mizikovsky for the purpose of improving the security of the system by updating the key periodically so that any compromised key wont be used on the system for long.

a. Referring to claim 7:

Regarding claim 7, the combination of Halasz and Mizikovsky teaches the method of claim 1 wherein in order to achieve encryption communication with the new key, when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically (See Mizikovsky, Col 12, Line 47-54 teaches periodically updating

Art Unit: 2432

the key) through the following steps of:

(a2) said AP generating a new key in any way and encrypting said new key with the present key (See Mizikovsky, Col 10, Line 50-65 teaches generating a new key which is a cryptographic function a random number and the present key);

(b2) said AP adding the encrypted key to the key update message and then sending said message to said mobile host (See Mizikovsky, Col 10, Line 43-45 teaches providing the unit with the SSD key);

(c2) when receiving said key update message, said mobile host decrypting the new key contained in said key update message with the present key so as to obtain said new key (See Mizikovsky, Col 11, Line 10-14 teaches receiving the update key message and obtaining the new key in a manner used by the system to generate the key);

(d2) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed (See Mizikovsky, Col 12, Line 17-54 teaches communications between the unit and the system encrypted with the encryption key and the unit. An encryption identifier, the encryption key is included in the message and the encryption key is changed whenever there is a key update); and

(e2) when receiving the data packets from said mobile host, said AP determines whether to change the key value of said encryption identifier (See Mizikovsky, Col 12, Line 39-43 teaches between the mobile node and the system and Line 47-50 further teaches the system determining whether to update the key value based on certain criteria).

Art Unit: 2432

a. Referring to claim 8:

Regarding claim 8, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 1, wherein when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically (See Mizikovsky, Col 12, Line 47-54 teaches periodically updating the key) through the following steps of:

(a3) said authentication device generating a random number which is used to generate a new key with the key generation algorithm, and then said authentication device sending said new key to AP, and sending said random number to said mobile host via AP (See Mizikovsky, Col 10, Line 33-66 teaches generating a random number which is used to generate a new key and sending the random number to the mobile unit);

(b3) said AP sending said key update message to said mobile host after receiving said new key (See Mizikovsky, Col 10, Line 33-50 teaches providing a key update message to the mobile unit);

(c3) when receiving said random number from said authentication device and said key update message from AP, said mobile host generating a new key from said random number with the same key generation algorithm as that in step (a3) (See Mizikovsky, Col 11, Line 10-29 teaches the mobile node generating a new key from the random number with the same key generation algorithm as that in step a3);

(d3) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier

Art Unit: 2432

to indicate the communication key has been changed (See Mizikovsky, Col 12, Line 17-54 teaches communications between the unit and the system encrypted with the encryption key and the unit. An encryption identifier, the encryption key is included in the message and the encryption key is changed whenever there is a key update); and

(e3) when receiving the data packets from said mobile host, said AP determines whether to change the key value of said encryption identifier (See Mizikovsky, Col 12, Line 39-43 teaches between the mobile node and the system and Line 47-50 further teaches the system determining whether to update the key value based on certain criteria).

a. Referring to claim 9:

Regarding claim 9, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in WLAN of claim 1, wherein in order to achieve encryption communication with the new key, when receiving the data packets encrypted with the key sent from said mobile host, said AP updates the key periodically or aperiodically (See Mizikovsky, Col 12, Line 47-54 teaches periodically updating the key) through the following steps of:

(a4) said AP generating a new key in any way and encrypting said new key with the present key, then sending said new key to said AP, whereas sending the encrypted new key to said mobile host via said AP (See Mizikovsky, Col 10, Line 50-65 teaches generating a new key which is a cryptographic function a random number and the present key and providing the key to the mobile host) ;

(b4) after receiving said new key, said AP sending a key update message to said mobile host (See Mizikovsky, Col 11, Line 10-11 teaches the mobile unit receiving a SSD update message sent from the system);

Art Unit: 2432

(c4) when receiving the encrypted key from said authentication device and said key update message from said AP, said mobile host decrypting the encrypted key with the present key to obtain a new key (See Mizikovsky, Col 11, Line 10-14 teaches receiving the update key message and obtaining the new key in a manner used by the system to generate the key);

(d4) said mobile host encrypting the data packets to be sent to AP with said new key and then sending the encrypted data packets to AP, during the encryption process, said mobile host adding an encryption identifier to said data packets and changing the value of said encryption identifier to indicate the communication key has been changed (See Mizikovsky, Col 12, Line 17-54 teaches communications between the unit and the system encrypted with the encryption key and the unit. An encryption identifier, the encryption key is included in the message and the encryption key is changed whenever there is a key update); and

(e4) when receiving the data packets from said mobile host, said AP determines whether to change the key value of said encryption identifier (See Mizikovsky, Col 12, Line 39-43 teaches between the mobile node and the system and Line 47-50 further teaches the system determining whether to update the key value based on certain criteria).

a. Referring to claim 11:

Regarding claim 11, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 6 wherein said authentication device is an authentication server installed in external network (See Halasz, Fig 1a. AS 106).

a. Referring to claim 12:

Art Unit: 2432

Regarding claim 12, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 7 wherein said authentication device is an authentication server installed in external network (See Halasz, Fig 1a. AS 106).

a. Referring to claim 13:

Regarding claim 13, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 8 wherein said authentication device is an authentication server installed in external network (See Halasz, Fig 1a. AS 106)

a. Referring to claim 14:

Regarding claim 14, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 9 wherein said authentication device is an authentication server installed in external network (See Halasz, Fig 1a. AS 106).

a. Referring to claim 16:

Regarding claim 16, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 6 wherein said authentication device is a wireless gateway that connects said AP with external network (See Halasz, Fig 1a, Switch and authenticator 100).

a. Referring to claim 17:

Regarding claim 17, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 7 wherein said authentication device is a wireless gateway that connects said AP with external network (See Halasz, Fig 1a, Switch and authenticator 100).

a. Referring to claim 18:



Art Unit: 2432

Regarding claim 18, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 8 wherein said authentication device is a wireless gateway that connects said AP with external network (See Halasz, Fig 1a, Switch and authenticator 100).

a. Referring to claim 19:

Regarding claim 19, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 9 wherein said authentication device is a wireless gateway that connects said AP with external network (See Halasz, Fig 1a, Switch and authenticator 100).

a. Referring to claim 21:

Regarding claim 21, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 6 wherein said authentication device includes said wireless gateway and said authentication server installed in external network (See Halasz, Fig 1a, AS 106 and Switch and authenticator 100).

a. Referring to claim 22:

Regarding claim 22, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 7 wherein said authentication device includes said wireless gateway and said authentication server installed in external network (See Halasz, Fig 1a, AS 106 and Switch and authenticator 100).

a. Referring to claim 23:

Regarding claim 23, the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 8 wherein said authentication device includes

Art Unit: 2432

said wireless gateway and said authentication server installed in external network (See Halasz, Fig 1a, AS 106 and Switch and authenticator 100).

a. Referring to claim 24:

Regarding claim 24 the combination of Halasz and Mizikovsky teaches the method for distributing encryption keys in the WLAN of claim 9 wherein said authentication device includes said wireless gateway and said authentication server installed in external network (See Halasz, Fig 1a, AS 106 and Switch and authenticator 100).

***Conclusion***

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to IZUNNA OKEKE whose telephone number is (571)270-3854. The examiner can normally be reached on 9:00am - 5:00pm.

Art Unit: 2432

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571) 272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/I. O./

Examiner, Art Unit 2432

/Gilberto Barron Jr./

Supervisory Patent Examiner, Art Unit 2432